PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-311114
(43)Date of publication of application : 07.11.2000

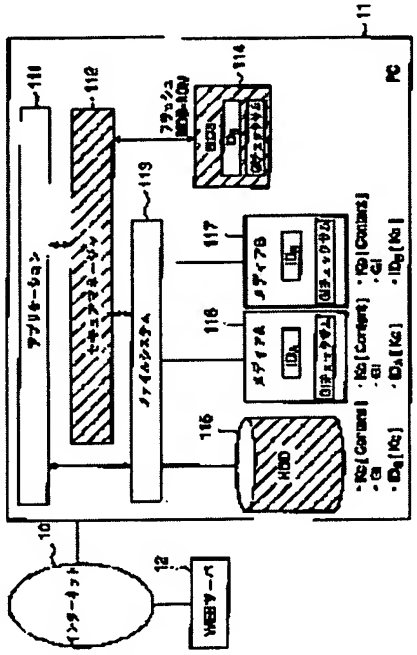
(51)Int.CI. G06F 12/14

(21)Application number : 11-122001
(22)Date of filing : 28.04.1999

(71)Applicant : TOSHIBA CORP
(72)Inventor : ISHIBASHI YASUHIRO
KAMIBAYASHI TATSU
TAMURA MASABUMI

(54) COMPUTER SYSTEM AND CONTENTS PROTECTING METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To make compatible the utilization and protection of digital contents by protecting the contents from illegal use even when these contents are recorded on an open recording medium such as hard disk drive.
SOLUTION: When using recording media 116 and 117 having medium ID, a secure manager 112 manages encoding/decoding of contents while using these medium ID. When using an HDD 115 having no medium ID, on the other hand, the secure manager 112 acquires a device ID peculiar to a system through a BIOS and manages encoding/decoding of contents recorded on the HDD 115 while using the device ID. The device ID is stored in a safe area inside a computer system.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－311114
（Ｐ2000－311114Ａ）
(43)公開日　平成12年11月７日(2000.11.7)

(51)Int.Cl.[7]	識別記号	ＦＩ	ﾃｰﾏｺｰﾄﾞ(参考)
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ　５Ｂ０１７

審査請求　未請求　請求項の数14　ＯＬ　（全 10 頁）

(21)出願番号　特願平11－122001

(22)出願日　平成11年４月28日(1999.4.28)

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　石橋　泰博
東京都青梅市末広町２丁目９番地　株式会社東芝青梅工場内

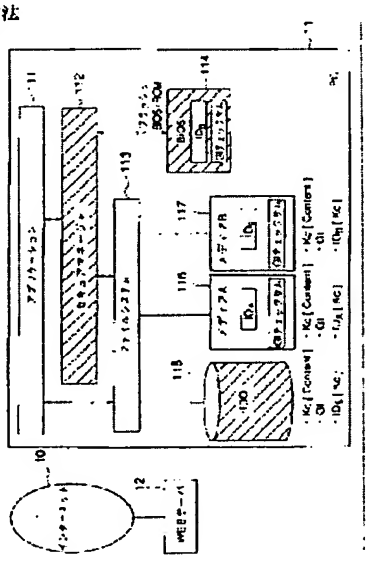
(72)発明者　上林　逸
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　100058479
弁理士　鈴江　武彦　（外６名）

最終頁に続く

(54)【発明の名称】　コンピュータシステムおよびコンテンツ保護方法

(57)【要約】
【課題】ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようにし、デジタルコンテンツの利用と保護の両立を図る。
【解決手段】セキュアマネージャ１１２は、メディアＩＤを有する記録メディア１１６，１１７を使用する場合には、コンテンツを記録する記録メディア毎にそのメディアＩＤを用いてコンテンツの暗号化／復号化の管理を行う。一方、メディアＩＤを持たないＨＤＤ１１５を使用する場合には、セキュアマネージャ１１２は、ＢＩＯＳを介してシステム 固有のデバイスＩＤを取得し、そのデバイスＩＤを用いて、ＨＤＤ１１５に記録するコンテンツの暗号化／復号化を管理する。デバイスＩＤはコンピュータシステム 内の安全な領域に記憶されている。



【特許請求の範囲】
【請求項 1】　コンテンツの安全管理のために使用されるデバイスＩＤを記憶するデバイスＩＤ記憶手段と、コンテンツを記録すべき記録メディア毎にその記録メディアが有するメディアＩＤを用いて前記コンテンツの暗号化／復号化を管理することが可能なコンテンツ管理手段であって、前記メディアＩＤを持たない記録メディアにコンテンツを記録する場合には、前記デバイスＩＤを用いて前記コンテンツの暗号化／復号化を管理するコンテンツ管理手段とを具備することを特徴とするコンピュータシステム。
【請求項 2】　前記デバイスＩＤ記憶手段のデバイスＩＤは、前記コンピュータシステムのＢＩＯＳによって管理されており、
前記コンテンツ管理手段は、前記ＢＩＯＳとの認証によって、前記デバイスＩＤを前記ＢＩＯＳから取得することを特徴とする請求項 1記載のコンピュータシステム。
【請求項 3】　前記デバイスＩＤ記憶手段は前記ＢＩＯＳを格納するためのＢＩＯＳ－ＲＯＭから構成されており、
前記ＢＩＯＳ－ＲＯＭはユーザからはアクセスできない安全な領域を有しており、その領域に前記デバイスＩＤが格納されていることを特徴とする請求項 2記載のコンピュータシステム。
【請求項 4】　前記コンテンツにはそのコンテンツの再生／コピー／移動を制限するための制御情報が付加されており、
前記ＢＩＯＳは前記制御情報の改変検出用のコードデータを管理し、
コンテンツ管理手段は、前記メディアＩＤを持たない記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記コンテンツと一緒に前記記録メディアに記録されている前記制御情報と、前記ＢＩＯＳによって管理されている前記改変検出用コードデータとに基づいて、前記要求された処理の実行を許可または禁止することを特徴とする請求項 2記載のコンピュータシステム。
【請求項 5】　前記コンテンツ管理手段は、前記メディアＩＤを持たない記録メディアに記録されているコンテンツを他の記録メディアにコピーする場合には、前記コンテンツのコピー可能回数の値が－１減少するように前記メディアＩＤを持たない記録メディア内の制御情報を更新すると共に、前記メディアＩＤを持たない記録メディアに記録されているコンテンツと前記更新後の制御情報を前記他の記録メディアにコピーし、且つ更新後の制御情報に基づいて前記ＢＩＯＳによって管理されている改変検出用コードデータの値を更新することを特徴とする請求項 4記載のコンピュータシステム。
【請求項 6】　前記コンテンツ管理手段は、前記メディアＩＤを持たない記録メディアに記録されているコンテンツを他の記録メディアに移動する場合には、前記メディアＩＤを持たない記録メディアに記録されている制御情報およびコンテンツを前記他の記録メディアに移動した後、前記メディアＩＤを持たない記録メディアに記録されているコンテンツおよびコピー制御情報を削除することを特徴とする請求項 4記載のコンピュータシステム。
【請求項 7】　前記コンテンツ管理手段は、前記メディアＩＤを持たない記録メディアに記録されているコンテンツに対して他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたとき、前記デバイスＩＤを用いて前記コンテンツまたはその暗号化鍵の暗号化を解除した後、コピー先または移動先の他の記録メディアのメディアＩＤを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を再度暗号化して前記他の記録メディアに記録することを特徴とする請求項 5または６記載のコンピュータシステム。
【請求項 8】　コンテンツを扱うことが可能なコンピュータシステムにおいて、
前記コンテンツの安全管理を行うコンテンツ管理手段を具備し、
前記コンテンツ管理手段は、
メディアＩＤを有する記録メディアにコンテンツを記録する場合には、前記メディアＩＤを用いて前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアＩＤを有する記録メディアに記録し、
メディアＩＤを持たない記録メディアにコンテンツを記録する場合には、前記コンピュータシステムのＢＩＯＳによって管理されている前記コンピュータシステムに固有のデバイスＩＤを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアＩＤを持たない記録メディアに記録することを特徴とするコンピュータシステム。
【請求項 9】　コンピュータシステムのハードウェア制御のためのシステムプログラムを有するコンピュータシステムにおいて、
前記システムプログラムによって管理されている前記コンピュータシステムに固有のデバイスＩＤを用いて、前記コンピュータシステムの記録メディアに記録すべきコンテンツの暗号化／復号化を管理するコンテンツ管理手段を具備することを特徴とするコンピュータシステム。
【請求項 １０】　前記コンテンツにはそのコンテンツの再生／コピー／移動を制限するための制御情報が付加されており、
前記システムプログラムは、前記制御情報の改変検出用のコードデータを管理し、
前記コンテンツ管理手段は、前記記録メディアに記録されているコンテンツの再生、他の記録メディアへのコピー、または他の記録メディアへの移動が要求されたと

き、前記コンテンツと一緒に前記記録メディアに記録されている前記制御情報と、前記システム プログラム によって管理されている前記改変検出用コードデータとに基づいて、前記要求された処理の実行を許可または禁止することを特徴とする請求項９記載のコンピュータシステム。

【請求項 １１】 コンピュータシステム に固有のデバイスＩＤを有するコンピュータシステム において、
前記コンピュータシステム からデバイスＩＤを取得し、その取得したデバイスＩＤを用いて、前記コンピュータシステム の記録メディアに記録すべきコンテンツの暗号化／復号化を管理するコンテンツ管理手段を具備することを特徴とするコンピュータシステム。

【請求項 １２】 コンテンツを扱うことが可能なコンピュータシステム に適用され、前記コンテンツを不正使用から保護するためのコンテンツ保護方法であって、
メディアＩＤを有する記録メディアにコンテンツを記録する場合には、前記メディアＩＤを用いて前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアＩＤを有する記録メディアに記録し、
メディアＩＤを持たない記録メディアにコンテンツを記録する場合には、前記コンピュータシステム 内のＢＩＯＳによって管理されている前記コンピュータシステム に固有のデバイスＩＤを用いて、前記コンテンツまたはそのコンテンツの暗号化鍵を暗号化して前記メディアＩＤを持たない記録メディアに記録することを特徴とするコンテンツ保護方法。

【請求項 １３】 システム 固有のデバイスＩＤを有するコンピュータシステム で扱われるコンテンツを不正使用から保護するためのコンテンツ保護方法であって、
前記コンピュータシステム から前記デバイスＩＤを取得し、
前記取得したデバイスＩＤを用いて、前記コンピュータシステム の記録メディアに記録すべきコンテンツの暗号化／復号化を管理することを特徴とするコンテンツ保護方法。

【請求項 １４】 コンピュータシステム で扱われるコンテンツを不正使用から保護するためのコンテンツ保護方法であって、
前記コンピュータシステム のハードウェア制御のためのシステム プログラム によって前記コンピュータシステムに固有のデバイスＩＤを管理しておき、
前記システム プログラム から前記デバイスＩＤを取得し、
前記取得したデバイスＩＤを用いて、前記コンピュータシステム の記録メディアに記録すべきコンテンツの暗号化／復号化を管理することを特徴とするコンテンツ保護方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】 本発明はコンピュータシステム およびそのコンピュータシステム に適用されるコンテンツ保護方法に関する。

【０００２】

【従来の技術】 近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータが種々開発されている。この種のパーソナルコンピュータは、ネットを通じて画像データや音楽データなどの種々なデジタルコンテンツをダウンロードして使用することができる。

【０００３】 これらデジタルコンテンツは、ＭＰＥＧ２、ＭＰ３といったデジタル符号化技術の採用により、品質を落とすことなくダウンロードすることができる。このため、最近では、著作権 保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【０００４】

【発明が解決しようとする課題】 しかし、パーソナルコンピュータは基本的にオープンなアーキテクチャを有するシステム であるため、パーソナルコンピュータにおけるデジタルコンテンツの保護は実際上困難である。パーソナルコンピュータ上ではデジタルコンテンツはファイルとして扱われるが、ファイルのコピー／移動は基本的に自由に行うことができるからである。特に、パーソナルコンピュータのストレージデバイスとして使用されるハードディスクドライブについては、その仕様はオープンであり、ハードディスクドライブ上に記録されたデジタルコンテンツの秘匿化を図ることは困難である。このため、インターネットからダウンロードしたデジタルコンテンツを一旦ハードディスクドライブに記録した後は、そのデジタルコンテンツをハードディスクドライブから他のメディアに自由にコピーして使用することができてしまう。

【０００５】 本発明は上述の事情に鑑みてなされたものであり、ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようにし、デジタルコンテンツの利用と保護の両立を図ることが可能なコンピュータシステム およびコンテンツ保護方法を提供することを目的とする。

【０００６】

【課題を解決するための手段】 上述の課題を解決するため、本発明のコンピュータシステム は、コンテンツの安全管理のために使用されるデバイスＩＤを記憶するデバイスＩＤ記憶手段と、コンテンツを記録すべき記録メディア毎にその記録メディアが有するメディアＩＤを用いて前記コンテンツの暗号化／復号化を管理することが可能なコンテンツ管理手段であって、前記メディアＩＤを持たない記録メディアにコンテンツを記録する場合には、前記デバイスＩＤを用いて前記コンテンツの暗号化

／復号化を管理するコンテンツ管理手段とを具備することを特徴とする。

【０００７】このコンピュータシステムにおいては、同一記録メディアであれば、その記録メディアを別の機器に移動して使用しても自由な再生が可能となるように、コンテンツは各記録メディア毎に用意されたメディアＩＤを用いて暗号化して記録される。しかし、ハードディスクドライブのような仕様のオープンな記録メディアの場合には、その記録メディア自体にメディアＩＤを安全に記録することは出来ない。そこで、本発明では、メディアＩＤを持たない記録メディアにコンテンツを記録する場合には、コンピュータシステムに固有のデバイスＩＤを用いて、コンテンツまたはそのコンテンツの暗号化鍵を暗号化して記録するという構成を採用している。デバイスＩＤをコンピュータシステム内の安全な領域で管理することにより、メディアＩＤを持たない記録メディアについても、メディアＩＤを持つ専用の記録メディアを使用する場合と同様に、そこに記録されるコンテンツの保護を図ることができる。

【０００８】この場合、デバイスＩＤはＢＩＯＳによって管理し、コンテンツ管理手段は、ＢＩＯＳとの認証によってデバイスＩＤを取得するように構成することが好ましい。このようにＢＩＯＳとの認証によって初めてデバイスＩＤを取得できるようにすることにより、デバイスＩＤをより安全に管理することができる。

【０００９】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。

【００１０】図１には、本発明の一実施形態に係るパーソナルコンピュータ（ＰＣ）のシステム構成が示されている。このパーソナルコンピュータ（ＰＣ）１１は、画像データや音楽データなどの各種デジタルコンテンツを扱うことが可能なコンピュータシステムである。このパーソナルコンピュータ（ＰＣ）１１におけるコンテンツ保護の方法は、コンテンツを記録すべき記録メディア毎にその記録メディアのメディアＩＤを用いてコンテンツの暗号化／復号化を管理することを前提としている。これは、同一記録メディアであれば、その記録メディアを他のパーソナルコンピュータや電子機器で使用しても再生できるようにするためであり、コンテンツは各記録メディアに用意された専用のメディアＩＤを用いて暗号化して記録される。メディアＩＤを用いたコンテンツの暗号化／復号化の管理は、そのための専用のソフトウェアであるセキュアマネージャ１１２によって実行される。このセキュアマネージャ１１２はタンパ・レジスタント・ソフトウェアとして実現されている。タンパ・レジスタント・ソフトウェアとは、不正な内部解析や改竄などの攻撃に対して防衛機能を備えるソフトウェアを意味する。

【００１１】セキュアマネージャ１１２は図示のようにアプリケーションプログラム１１１とファイルシステム１１３との間に位置し、保護対象のコンテンツについての「記録」、「再生」、「コピー」、「移動」などの各種操作は、セキュアマネージャ１１２を介して行われる。セキュアマネージャ１１２によるコンテンツの暗号化／復号化管理は、１）専用のメディアＩＤを内蔵する記録メディアに対するものと、２）メディアＩＤを持たない通常の記録メディアに対するものとに、大別される。

【００１２】（メディアＩＤを有する記録メディア）まず、メディアＩＤを有する記録メディアに対する処理について説明する。

【００１３】記録メディア（Ａ）１１６、および記録メディア（Ｂ）１１７は、それぞれセキュアマネージャ１１２に対応した専用の記録メディアである。これら記録メディアとしては、パーソナルコンピュータ（ＰＣ）１１や他の各種電子機器に着脱自在に装着可能なメモリカードなどの各種媒体（ＳＳＦＤＣ、フラッシュＰＣカード、ミニディスク）などを使用することができる。

【００１４】記録メディア（Ａ）１１６には、通常のデータ記憶領域の他、その記録メディアに固有のメディアＩＤ（ＩＤA）が予め記憶されているＲＯＭ領域と、後述のＧＩ（Ｇｏｖｅｒｎａｎｃｅ　Ｉｎｆｏｒｍａｔｉｏｎ）テーブルから作成されたＧＩチェックサムデータを格納するためのＧＩチェックサム領域とが設けられている。記録メディア（Ｂ）１１７についても同様の構成である。メディアＩＤは各記録メディアに固有であれば良く、シリアル番号や製造番号、他の様々な識別情報を利用することができる。

【００１５】ＧＩテーブルとは、保護対象の各コンテンツ毎にその再生、コピー、移動の可否、およびコピー可能回数、移動可能回数などを規定したコピー制御情報である。ＧＩチェックサムデータはＧＩテーブルの内容の改竄を検出するための改変検出用コードデータであり、ＧＩテーブルの値から算出される。ＧＩチェックサムデータの代わりにＧＩテーブルのハッシュ値を用いることもできる。ＧＩテーブルの「コピー可能回数」の値は、コピーが実行される度に－１減算される。このようにＧＩテーブルの値が更新される度に、その更新に合わせて、ＧＩチェックサムデータの値も更新される。このため、ＧＩチェックサム領域は書き換え可能な領域から構成されている。

【００１６】ＲＯＭ領域およびＧＩチェックサム領域のどちらも、ユーザからはアクセスできないセキュアな領域となっている。

【００１７】コンテンツを記録メディア（Ａ）１１６に記録する場合には、セキュアマネージャ１１２は、記録メディア（Ａ）１１６のメディアＩＤを用いてコンテンツの暗号化／復号化を管理する。この場合、記録メディア（Ａ）１１６のデータ領域には、以下のデータが格納

される。
【００１８】・Ｋｃ［Ｃｏｎｔｅｎｔ］：　コンテンツキーＫｃと称される秘密鍵によって暗号化されたコンテンツ
・ＧＩ
・ＩＤＡ［Ｋｃ］：　記録メディア（Ａ）１１６のメディアＩＤ（ＩＤＡ）によって暗号化されたコンテンツキー
記録メディア（Ａ）１１６に記録されたコンテンツを再生する場合には、セキュアマネージャ１１２は、まず、記録メディア（Ａ）１１６のメディアＩＤ（ＩＤＡ）を用いてＩＤＡ［Ｋｃ］を復号化し、Ｋｃを得る。そして、そのＫｃによって、Ｋｃ［Ｃｏｎｔｅｎｔ］を復号化する。
【００１９】記録メディア（Ａ）１１６に記録されたコンテンツがコピー可能なコンテンツである場合、そのコンテンツを記録メディア（Ａ）１１６から他の記録メディア（例えば記録メディア（Ｂ）１１７）にコピーすることができる。この場合、セキュアマネージャ１１２は、記録メディア（Ａ）１１６に格納されたＧＩからチェックサム データを生成し、そのチェックサム データを、記録メディア（Ａ）１１６のＧＩチェックサム 領域のＧＩチェックサム データと比較する。不一致の場合には、コピーは禁止される。一致した場合には、セキュアマネージャ１１２は、記録メディア（Ａ）１１６のメディアＩＤ（ＩＤＡ）を用いてＩＤＡ［Ｋｃ］を復号化し、Ｋｃを得る。次いで、セキュアマネージャ１１２は、コピー先の記録メディア（Ｂ）１１７のメディアＩＤ（ＩＤＢ）を用いてＫｃを暗号化し、暗号化したコンテンツキー（ＩＤＢ［Ｋｃ］）を、Ｋｃ［Ｃｏｎｔｅｎｔ］およびＧＩと一緒に、記録メディア（Ｂ）１１７のデータ領域に書き込む。この場合、記録メディア（Ａ）１１６，記録メディア（Ｂ）１１７のどちらにおいても、ＧＩによって指定されるコピー可能回数の値は－１される。例えば、コピーしたコンテンツが「一回のみコピー可」のコンテンツであった場合には、「これ以上コピー不可」のコンテンツに変更される。また、ＧＩの更新に伴い、記録メディア（Ａ）１１６，記録メディア（Ｂ）１１７それぞれのＧＩチェックサム データの値も更新される。
【００２０】記録メディア（Ａ）１１６に記録されたコンテンツが移動可能なコンテンツである場合、そのコンテンツを記録メディア（Ａ）１１６から他の記録メディア（例えば記録メディア（Ｂ）１１７）に移動することができる。この場合、セキュアマネージャ１１２は、記録メディア（Ａ）１１６に格納されたＧＩからチェックサム データを生成し、そのチェックサム データを、記録メディア（Ａ）１１６のＧＩチェックサム 領域のＧＩチェックサム データと比較する。不一致の場合には、移動は禁止される。一致した場合には、セキュアマネージャ１１２は、記録メディア（Ａ）１１６のメディアＩＤ（ＩＤＡ）を用いてＩＤＡ［Ｋｃ］を復号化し、Ｋｃを得る。次いで、セキュアマネージャ１１２は、移動先の記録メディア（Ｂ）１１７のメディアＩＤ（ＩＤＢ）を用いてＫｃを暗号化し、暗号化したコンテンツキー（ＩＤＢ［Ｋｃ］）を、Ｋｃ［Ｃｏｎｔｅｎｔ］およびＧＩと一緒に、記録メディア（Ｂ）１１７のデータ領域に書き込む。この後、セキュアマネージャ１１２は、移動元の記録メディア（Ａ）１１６のデータ領域に格納されているＫｃ［Ｃｏｎｔｅｎｔ］、ＧＩ、ＩＤＡ［Ｋｃ］を削除すると共に、ＧＩチェックサム 領域のＧＩチェックサム データを削除する。ＧＩによって規定されているのが「コピー可能回数」のみで、「移動可能回数」については規定されていない場合には、移動によるＧＩの更新は行われない。「移動可能回数」が規定されている場合には、前述の「コピー」の場合と同様にして、ＧＩは更新された後に記録メディア（Ｂ）１１７に書き込まれ、またその更新後のＧＩに対応するチェックサム データがＧＩチェックサム 領域に書き込まれることになる。
【００２１】（メディアＩＤを持たない記録メディア）
次に、メディアＩＤを持たない記録メディアに対する処理について説明する。ＨＤＤ１１５はパーソナルコンピュータ（ＰＣ）１１の二次記憶装置として使用されるストレージデバイスであり、パーソナルコンピュータ（ＰＣ）１１に固定されて使用される。ＨＤＤ１１５には、記録メディア（Ａ）１１６、および記録メディア（Ｂ）１１７のようなＲＯＭ領域やＧＩチェックサム 領域は設けられていない。
【００２２】ＨＤＤ１１５を用いてコンテンツの記録、コピー、移動などを行う場合、セキュアマネージャ１１２は、メディアＩＤの代わりに、本パーソナルコンピュータ（ＰＣ）１１に固有のデバイスＩＤを用いて、コンテンツの暗号化／復号化の管理を行う。つまり、セキュアマネージャ１１２は、コンテンツの記録先、コピー先、コピー元、移動先、または移動元がＨＤＤ１１５に対応するドライブ番号であった場合には、メディアＩＤではなく、システム 内で管理されているデバイスＩＤを使用する。この場合、どのドライブ番号の記録メディアがメディアＩＤを持ち、どのドライブ番号の記録メディアがメディアＩＤを持たないかは、例えば、プラグアンドプレイ等の機能を利用することにより、セキュアマネージャ１１２がメディア毎に認識できるようにすることもできる。
【００２３】ＰＣ１１固有のデバイスＩＤは、ＰＣ１１のハードウェア制御のためのシステム プログラム である ＢＩＯＳによって管理されている。ＢＩＯＳは、そのＢＩＯＳ自体のアップデートに対応するために、書き換え可能な不揮発性メモリから構成されたフラッシュＢＩＯＳ－ＲＯＭ１１４に格納されている。フラッシュＢＩＯＳ－ＲＯＭ１１４はユーザからはアクセスできないセキ

ュアな領域を有しており、そこには、図２に示すように、パスワードエリアに加え、ＩＤエリア、チェックサム エリアなどが設けられている。パスワードエリアは、ユーザによって登録されたパスワードを記憶するための領域である。パスワードが登録されている場合には、電源投入時にユーザからの入力パスワードと登録パスワードとの一致の有無が判定され、一致した場合にのみ、ＯＳのブートや、サスペンド／ハイバネーション状態からの復帰が可能となる。

【００２４】ＩＤエリアには、ＰＣ１１に固有のデバイスＩＤ（ＩＤＳ）が予め記憶されている。チェックサムエリアは、ＨＤＤ１１５に記憶されるコンテンツのＧＩから作成されたＧＩチェックサム データの格納に用いられる。

【００２５】ＢＩＯＳには、セキュアマネージャ１１２との間で認証処理を行うための認証機能が設けられている。セキュアマネージャ１１２とＢＩＯＳとの認証処理により、互いに正しいプログラム 同士であ ることが確認されると、セキュアマネージャ１１２は、ＢＩＯＳからデバイスＩＤ（ＩＤＳ）を取得することができる。このようにＢＩＯＳとの認証によって初めてデバイスＩＤを取得できるようにすることにより、デバイスＩＤをより安全に管理することができる。

【００２６】次に、図３および図５を参照して、ＨＤＤ１１５を使用する場合のコンテンツ管理処理の手順について具体的に説明する。

【００２７】「記録」図３はコンテンツ記録時の動作の流れを示している。

【００２８】（ステップ１）：　ＰＣ１１の起動時には、まず、セキュアマネージャ１１２とＢＩＯＳとの間で認証処理が実行される。互いに正しいプログラム 同士であ ることが確認されると、セキュアマネージャ１１２とＢＩＯＳとの間でキー交換が行われ、同一の認証鍵（Kx2）が共有される。認証鍵（Kx2）は、毎回代わる時変キーであ る。

【００２９】（ステップ２）：　セキュアマネージャ１１２は、ＩＤ取得要求をＢＩＯＳに発行する。セキュアマネージャ１１２からのＩＤ取得要求に応答して、ＢＩＯＳは、デバイスＩＤ（ＩＤＳ）を認証鍵（Kx2）で暗号化し、暗号化されたデバイスＩＤ（Kx2［ＩＤＳ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Kx2）を保持しているので、Kx2［ＩＤＳ］からＩＤＳ を解読することができる。

【００３０】（ステップ３）：　ＷＥＢブラウザなどのアプリケーションプログラム を用いてＷＥＢサーバから画像データや音楽データなどのコンテンツをダウンロードする場合には、ＷＥＢブラウザを介して、あ るいは直接、セキュアマネージャ１１２とＷＥＢサーバ１２との間で認証処理が行われる。互いに正しいコンテンツ保護機能を有するもの同士あ ることが確認されると、セキュアマネージャ１１２とＷＥＢサーバ１２との間でキー交換が行われ、同一の認証鍵（Kx1）が共有される。認証鍵（Kx1）は毎回代わる時変キーであ る。

【００３１】（ステップ４）：　ＷＥＢサーバ１２は、要求されたコンテンツを所定のコンテンツキーＫｃで暗号化したもの（Kc［Ｃｏｎｔｅｎｔ］）と、認証鍵（Kx1）で暗号化したコンテンツキー（Kx1［Ｋｃ］）と、ＧＩとを、ＰＣ１１宛に送信する。

【００３２】（ステップ５）：　これら、Ｋｃ［Ｃｏｎｔｅｎｔ］、Kx1［Ｋｃ］、ＧＩは、ＷＥＢブラウザなどを介して、セキュアマネージャ１１２に送られる。セキュアマネージャ１１２は、ＷＥＢブラウザから指定されたダウンロード先の記録メディアがＨＤＤ１１５である場合、認証鍵（Kx1）と、ＢＩＯＳから取得したデバイスＩＤ（ＩＤＳ）を用いて、Kx1［Ｋｃ］をＩＤＳ［Ｋｃ］に変換する。この場合、まず、認証鍵（Kx1）を用いてKx1［Ｋｃ］がＫｃに復号化され、そのＫｃがあ らためてＩＤＳ によって暗号化される。

【００３３】この後、セキュアマネージャ１１２は、Ｋｃ［Ｃｏｎｔｅｎｔ］、ＩＤＳ［Ｋｃ］、ＧＩをファイルシステム １１３、さらにはＩＤＥドライバなどを通して、ＨＤＤ１１５に書き込む。

【００３４】（ステップ６）：　セキュアマネージャ１１２は、ＧＩからＧＩチェックサム データ（ＧＩ＿ＣＳ）を算出し、それをＢＩＯＳとの認証鍵（Kx2）で暗号化してＢＩＯＳに渡す。ＢＩＯＳは、ＧＩチェックサム データを暗号化されたまま、あ るいは復号化した後に、フラッシュＢＩＯＳ＿ＲＯＭ１１４のチェックサム エリアに書き込む。もちろん、セキュアマネージャ１１２が直接フラッシュＢＩＯＳ＿ＲＯＭ１１４のチェックサム エリアに、ＧＩチェックサム データあ るいはその暗号化データを書き込むようにしても良い。

【００３５】「再生」図４はコンテンツ再生時の動作の流れを示している。

【００３６】（ステップ１）：　ＰＣ１１の起動時には、まず、セキュアマネージャ１１２とＢＩＯＳとの間で認証処理が実行される。互いに正しいプログラム 同士であ ることが確認されると、セキュアマネージャ１１２とＢＩＯＳとの間でキー交換処理が行われ、同一の認証鍵（ここでは、Kx1とする）が共有される。認証鍵（Kx1）は毎回代わる時変キーであ る。

【００３７】（ステップ２）：　セキュアマネージャ１１２からのＩＤ取得要求に応答して、ＢＩＯＳは、デバイスＩＤ（ＩＤＳ）を認証鍵（Kx1）で暗号化し、暗号化されたデバイスＩＤ（Kx1［ＩＤＳ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Kx1）を保持しているので、Kx1［ＩＤＳ］からＩＤＳ を解読することができる。

【００３８】（ステップ３）：　次に、セキュアマネージャ１１２からのＧＩチェックサム データの取得要求に

応答して、ＢＩＯＳは、ＧＩチェックサム データ（ＧＩ＿ＣＳ）を認証鍵（Ｋx1）で暗号化し、暗号化されたＧＩチェックサム データ（Ｋx1［ＧＩ＿ＣＳ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Ｋx1）を保持しているので、Ｋx1［ＧＩ＿ＣＳ］からＧＩ＿ＣＳを解読することができる。

【００３９】（ステップ４）：　セキュアマネージャ１１２は、アプリケーションプログラム １１１などから指定された再生対象の暗号化されたコンテンツ（（Ｋｃ［Ｃｏｎｔｅｎｔ］）と、それに対応するＩＤＳ［Ｋｃ］、およびＧＩを、ファイルシステム １１３、さらにはＩＤＥドライバなどを介して、ＨＤＤ１１５から取得する。

【００４０】（ステップ５）：　セキュアマネージャ１１２は、ＧＩからチェックサム を算出し、その算出したチェックサム と、ＢＩＯＳから取得したＧＩ＿ＣＳとを比較する。不一致の場合には、ＨＤＤ１１５のＧＩが悪意を持つユーザによって書き替えられた恐れがあ るため、再生処理はこの時点で中止する。一致した場合には、セキュアマネージャ１１２は、ＢＩＯＳから取得したＩＤＳ を用いて、ＩＤＳ［Ｋｃ］を復号し、Ｋｃを得る。そして、そのＫｃを用いてＫｃ［Ｃｏｎｔｅｎｔ］の暗号を解除し、生のコンテンツ（Ｃｏｎｔｅｎｔ）を再生ソフト（プレイヤ）に送信する。再生ソフトもタンパ・レジスタント・ソフトウェアとして実現されている。

【００４１】「コピー」図５はコンテンツコピー時の動作の流れを示している。ここでは、ＨＤＤ１１５に記録されているコンテンツを記録メディア（Ａ）１１６にコピーする場合を例示する。

【００４２】（ステップ１）：　ＰＣ１１の起動時には、まず、セキュアマネージャ１１２とＢＩＯＳとの間で認証処理が実行される。互いに正しいプログラム 同士であ ることが確認されると、セキュアマネージャ１１２とＢＩＯＳとの間でキー交換処理が行われ、同一の認証鍵（ここでは、Ｋx1とする）が共有される。認証鍵（Ｋx1）は毎回代わる時変キーであ る。

【００４３】（ステップ２）：　セキュアマネージャ１１２からのＩＤ取得要求に応答して、ＢＩＯＳは、デバイスＩＤ（ＩＤＳ）を認証鍵（Ｋx1）で暗号化し、暗号化されたデバイスＩＤ（Ｋx1［ＩＤＳ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Ｋx1）を保持しているので、Ｋx1［ＩＤＳ］からＩＤＳ を解読することができる。

【００４４】（ステップ３）：　次に、セキュアマネージャ１１２からのＧＩチェックサム データの取得要求に応答して、ＢＩＯＳは、ＧＩチェックサム データ（ＧＩ＿ＣＳ）を認証鍵（Ｋx1）で暗号化し、暗号化されたＧＩチェックサム データ（Ｋx1［ＧＩ＿ＣＳ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Ｋx1）を保持しているので、Ｋx1［ＧＩ＿ＣＳ］からＧＩ＿ＣＳを解読することができる。

【００４５】（ステップ４）：　セキュアマネージャ１１２は、アプリケーションプログラム １１１などから指定されたコピー対象の暗号化されたコンテンツ（（Ｋｃ［Ｃｏｎｔｅｎｔ］）と、それに対応するＩＤＳ［Ｋｃ］、およびＧＩを、ファイルシステム １１３、さらにはＩＤＥドライバなどを介して、ＨＤＤ１１５から取得する。

【００４６】セキュアマネージャ１１２は、ＧＩからチェックサム を算出し、その算出したチェックサム と、ＢＩＯＳから取得したＧＩ＿ＣＳとを比較する。不一致の場合には、ＨＤＤ１１５のＧＩが悪意を持つユーザによって書き替えられた恐れがあ るため、コピー処理はこの時点で中止する。一致した場合には、ＨＤＤ１１５のＧＩを参照して、コピー対象のコンテンツがコピー可能なコンテンツであ るか否かを調べる。「コピー不可」または「コピー可能回数＝零」の場合には、コピー処理はこの時点で中止する。コピーが許されたコンテンツであ れば、セキュアマネージャ１１２は、次のステップ５以降の処理に進む。

【００４７】（ステップ５）：　セキュアマネージャ１１２は、コピー先の記録メディア（Ａ）１１６またはそれを制御するためのデバイスドライバとの間で認証処理を行う。互いに正しいコンテンツ保護機能をもつもの同士であ ることが確認されると、セキュアマネージャ１１２とコピー先の記録メディア（Ａ）１１６またはそのデバイスドライバとの間でキー交換が行われ、同一の認証鍵（ここでは、Ｋx2とする）が共有される。認証鍵（Ｋx2）は毎回代わる時変キーであ る。

【００４８】（ステップ６）：　セキュアマネージャ１１２からのＩＤ取得要求に応答して、記録メディア（Ａ）１１６またはそのデバイスドライバは、メディアＩＤ（ＩＤＡ）を認証鍵（Ｋx2）で暗号化し、暗号化されたメディアＩＤ（Ｋx2［ＩＤＡ］）をセキュアマネージャ１１２に送信する。セキュアマネージャ１１２は、認証鍵（Ｋx2）を保持しているので、Ｋx2［ＩＤＡ］からＩＤＡ を解読することができる。

【００４９】（ステップ７）：　セキュアマネージャ１１２は、ＨＤＤ１１５から取得したＧＩを更新し、「コピー可能回数」が－１されたＧＩ′を得る。そして、ＢＩＯＳから取得したデバイスＩＤ（ＩＤＳ）を用いてＩＤＳ［Ｋｃ］を復号化し、Ｋｃを得る。次いで、セキュアマネージャ１１２は、ＫｃをメディアＩＤＡを用いて暗号化し、ＩＤＡ［Ｋｃ］を得る。この後、セキュアマネージャ１１２は、Ｋｃ［Ｃｏｎｔｅｎｔ］、ＩＤＡ［Ｋｃ］、ＧＩ′を、ファイルシステム １１３さらには記録メディア（Ａ）１１６のドライバなどを介して記録メディア（Ａ）１１６に書き込む。

【００５０】（ステップ８）：　セキュアマネージャ１

12は、ＧＩ′からそのチェックサム データ（ＧＩ′＿ＣＳ）を算出し、それを認証鍵（Ｋｘ2）で暗号化したもの（Ｋｘ2［ＧＩ′＿ＣＳ］）を記録メディア（Ａ）１１５またはそのドライバに送信し、ＧＩ′＿ＣＳを記録メディア（Ａ）１１５のＧＩチェックサム 領域に書き込む。

【００５１】（ステップ９）： この後、セキュアマネージャ１１２は、チェックサム データ（ＧＩ′＿ＣＳ）をＢＩＯＳとの認証鍵（Ｋｘ1）で暗号化し、それをＢＩＯＳに送信する。ＢＩＯＳは、フラッシュＢＩＯＳ＿ＲＯＭ１１４のチェックサム エリアの内容をＧＩ′＿ＣＳに書き換える。

【００５２】（ステップ１０）： そして、セキュアマネージャ１１２は、ＨＤＤ１１５のＧＩをＧＩ′に更新する。

【００５３】［移動］ＨＤＤ１１５に記録されているコンテンツを記録メディア（Ａ）１１５に移動する場合は、図５のコピー処理と基本的に同じ手順で処理が行われるが、ステップ９の代わりにフラッシュＢＩＯＳ＿ＲＯＭ１１４のチェックサム エリアの内容を削除する処理が行われ、また図５のステップ１０の代わりにＨＤＤ１１５のＫｃ［Ｃｏｎｔｅｎｔ］、ＩＤＳ［Ｋｃ］、およびＧＩを削除する処理が行われる、点がコピー処理とは異なる。また、移動の場合は、コピー可能回数に対するＧＩの更新は行われず、移動可能回数が規定されている場合を除き、ＧＩは更新されずに移動先の記録メディア（Ａ）１１５に書き込まれることになる。

【００５４】以上のように、本実施形態においては、ＢＩＯＳにセキュアマネージャ１１２との認証機能やデバイスＩＤ管理機能を持たせることにより、メディアＩＤを持たない記録メディアにコンテンツを記録する場合でも、メディアＩＤを持つ専用の記録メディアを使用する場合と同様に、そこに記録されるコンテンツの保護を図ることができる。特に、デバイスＩＤおよびＧＩチェックサム データをＢＩＯＳによって管理し、システム 側からはアクセスできないようにしているので、ＨＤＤ１１５に対して何ら変更を加えることなく、ＨＤＤ１１５にダウンロードしたコンテンツを不正使用から保護することができる。

【００５５】なお、本実施形態では、コンテンツの暗号化鍵であ るコンテンツキーをメディアＩＤやデバイスＩＤを用いて暗号化するようにしてが、メディアＩＤやデバイスＩＤをコンテンツキーとして使用し、コンテンツ自体をメディアＩＤやデバイスＩＤを用いて暗号化するようにしてもよい。また、メディアＩＤを持たない記憶メディアとしてＨＤＤを例示したが、デバイスＩＤを用いて暗号化／復号化の管理を行う本実施形態のコンテンツ保護方法は、例えば、ＭＯやメモリカードなど、メディアＩＤを持たない通常の記憶メディア全てに対して適用することができる。

【００５６】また、デバイスＩＤはＰＣ１１内の安全な記憶装置に記憶してあ ればよく、例えば、ＰＣ１１内の埋め込みコントローラ（ＥＣ）内に記憶したり、ＰＣ１１内に設けられているリアルタイム クロック内のバッテリバックアップされたＣＭＯＳメモリなどに記憶してもよい。ＰＣ１１内のどこにデバイスＩＤを記憶した場合でも、ＢＩＯＳを介してデバイスＩＤを取得するようにすることにより、セキュアマネージャ１１２はデバイスＩＤの記憶場所を意識することなく、必要な処理を行うことができる。

【００５７】さらに、本実施形態は、ＰＣに限らず、セットトップボックス、ゲーム 機、オーディオ／ビデオプレイヤーなど、マイクロプロセッサを搭載したあ らゆるデータ処理装置（コンピュータ応用機器）に適用することができる。

【００５８】また、セキュアマネージャ１１２の機能、つまり、前述したようにＢＩＯＳからデバイスＩＤを取得し、そのデバイスＩＤを用いてコンテンツの暗号化／復号化を管理する手順や、メディアＩＤを有する記録メディアについてはそのメディアＩＤを用いてコンテンツの暗号化／復号化を管理する手順などを含むコンピュータプログラム を通信媒体や記録媒体を介してコンピュータに導入することにより、ＢＩＯＳによってデバイスＩＤを管理することが可能なシステム であ れば、本実施形態と同様の効果を得ることができる。また、ＢＩＯＳについても、そのアップデートが可能であ るので、通常のハードウェア制御機能に加え、認証機能や、デバイスＩＤおよびその管理機能などを持つ新たなＢＩＯＳを通信媒体や記録媒体を介してコンピュータに導入すれば、既存のコンピュータにおいても本実施形態と同様の効果を得ることができる。

【００５９】

【発明の効果】以上説明したように、本発明によれば、ハードディスクドライブのようなオープンな記録メディアにコンテンツを記録した場合でもそのコンテンツを不正使用から保護できるようになり、デジタルコンテンツの利用と保護の両立を図ることが可能となる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るコンピュータシステム の基本構成を示すブロック図。

【図２】同実施形態のコンピュータシステム に設けられたフラッシュＢＩＯＳ＿ＲＯＭの記憶内容の一例を示す図。

【図３】同実施形態のコンピュータシステム で行われるコンテンツ記録処理の手順を示す図。

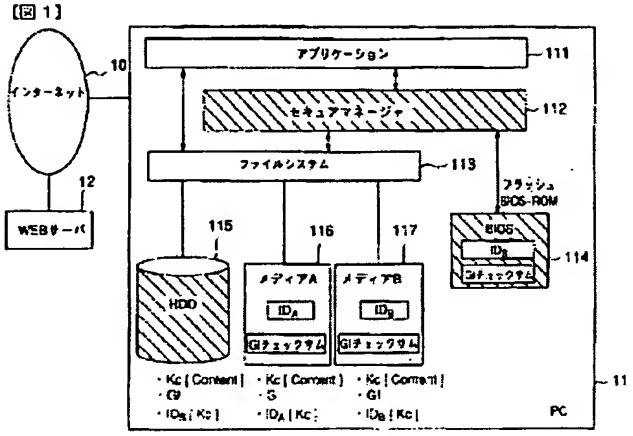
【図４】同実施形態のコンピュータシステム で行われるコンテンツ再生処理の手順を示す図。

【図５】同実施形態のコンピュータシステム で行われるコンテンツコピー処理の手順を示す図。

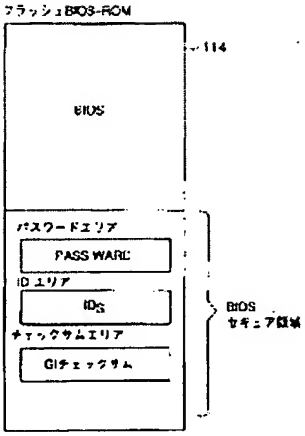
【符号の説明】

１０…インターネット
１１…パーソナルコンピュータ（ＰＣ）
１２…ＷＥＢサーバ
１１１…アプリケーションプログラム
１１２…セキュアマネージャ
１１３…ファイルシステム
１１４…フラッシュＢＩＯＳ＿ＲＯＭ
１１５…ＨＤＤ
１１６…記録メディア（Ａ）
１１７…記録メディア（Ｂ）

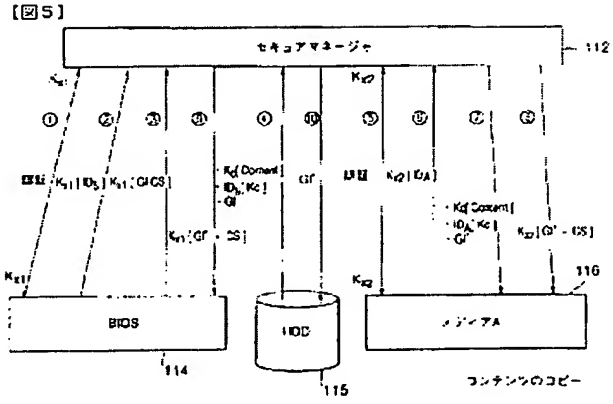
【図１】



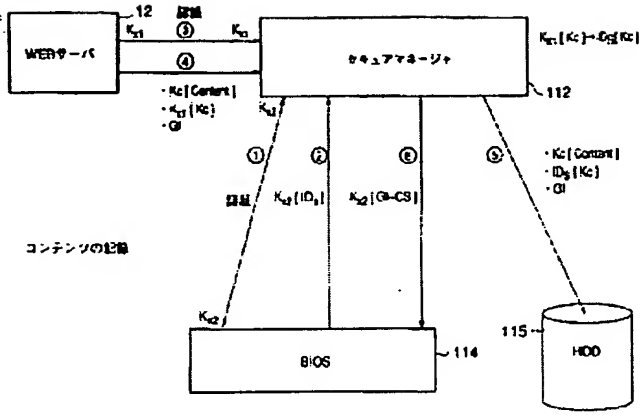
【図２】



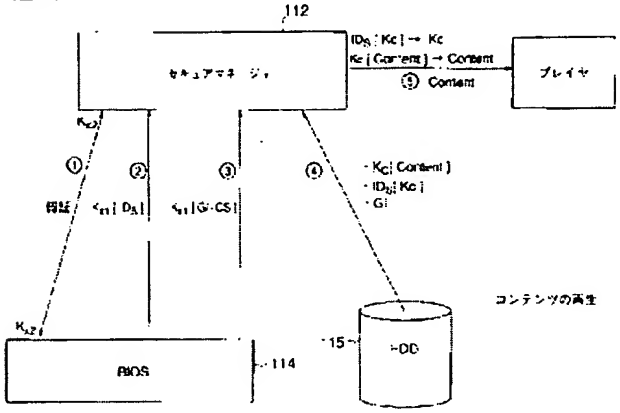
【図５】



【図３】



【図４】



フロントページの続き

(72)発明者　田村　正文
東京都港区芝浦一丁目１番１号　株式会社
東芝本社事務所内

Ｆターム（参考）　5B017 AA05 AA07 BA07 BB06 BB10
CA16